REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
20-05-2013	FINAL	

4. TITLE AND SUBTITLE
The Challenges of Defense Support of Civil Authorities and Homeland Defense in the Cyber Domain

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Christopher A. Hopes, MAJ, USA

Paper Advisors: CDR Chad Piacenti, USN & LtCol Larry Floyd, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES: A paper submitted to the Naval War College Faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

Defending U.S. National Critical Infrastructure and Key Resources (CIKR) and the Global Information Grid (GIG) against a cyber attack has taken the forefront in national level discussions. The U.S. homeland's assumed sanctuary against cyber disruption and cyber attack is often little more than an afterthought to defense planners. However, recent state and non-state adversarial threats have proved their strength and efficacy in the cyber domain by disrupting supply chains, attacking banking systems, seizing intellectual property, and compromising the software used to operate aspects of the CIKR. As a result, the Department of Defense (DoD) is challenged to provide support to other U.S. government agencies and key operators within the private sector to detect, deter, prevent, and thwart exploitation of CIKR and the GIG. U.S. Cyber Command (USCYBERCOM), a subordinate unified command of U.S. Strategic Command, is responsible for defending DoD information systems and networks. USCYBERCOM is also tasked to conduct Cyber Defense Support of Civil Authorities (DSCA), when directed by the President or Secretary of Defense. This paper discusses how USCYBERCOM's capabilities have synchronized and effectively arrayed resources into a functional interagency effort to improve cyber security for the nation. It identifies the complex challenges of conducting Cyber-DSCA in an interagency environment and the statutory authorities governing DoD operational elements. Furthermore, USCYBERCOM's formal establishment of a Standing Joint Task Force provides a structure for conducting these complex Cyber-DSCA operations.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					Chairman, JMO Dept
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		28	401-841-3556

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, RI

The Challenges of Defense Support of Civil Authorities and Homeland Defense in the Cyber Domain

by

Christopher A. Hopes

MAJ, USA

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

20 May 2013

Contents

Abstract

Defending U.S. National Critical Infrastructure and Key Resources (CIKR) and the Global Information Grid (GIG) against a cyber attack has taken the forefront in national level discussions. The U.S. homeland's assumed sanctuary against cyber disruption and cyber attack is often little more than an afterthought to defense planners. However, recent state and non-state adversarial threats have proved their strength and efficacy in the cyber domain by disrupting supply chains, attacking banking systems, seizing intellectual property, and compromising the software used to operate aspects of the CIKR. As a result, the Department of Defense (DoD) is challenged to provide support to other U.S. government agencies and key operators within the private sector to detect, deter, prevent, and thwart exploitation of CIKR and the GIG. U.S. Cyber Command (USCYBERCOM), a subordinate unified command of U.S. Strategic Command, is responsible for defending DoD information systems and networks. USCYBERCOM is also tasked to conduct Cyber Defense Support of Civil Authorities (DSCA), when directed by the President or Secretary of Defense. This paper discusses how USCYBERCOM's capabilities have synchronized and effectively arrayed resources into a functional interagency effort to improve cyber security for the nation. It identifies the complex challenges of conducting Cyber-DSCA in an interagency environment and the statutory authorities governing DoD operational elements. Furthermore, USCYBERCOM's formal establishment of a Standing Joint Task Force provides a structure for conducting these complex Cyber-DSCA operations.

Introduction

> *"The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats."* -Executive Order, February 2013[1]

The Executive Order shown above highlights a national security challenge that has been acknowledged by cyber security professional since the early 1980's. In 1983, the American public became more aware of the emerging world of computer hacking with the release of the movie *WarGames,* which portrayed a high school student who was able to hack into a computer system that controls nuclear weapons at the North American Aerospace Defense Command.[2] In the same timeframe, the actual intrusion of government computer systems, most notably the Los Alamos National Laboratory in 1983, prompted calls for congressional hearings to examine cyber threats to U.S. Government computer systems,[3] ultimately resulting in legislation such as the Computer Security Act of 1987. This act declared that "improving on the security and privacy of sensitive information in Federal computer systems is in the public's interest."[4] Later legislation including the Homeland Security Act of 2002[5] and the National Defense Authorization Act (NDAA) of 2012[6] have made progress to make U.S. National Critical Infrastructure and Key Resources (CIKR) and the Global Information Grid (GIG) more secure from cyber attack and exploitation.

Homeland Security Presidential Directive (HSPD)-7 broadly describes that "CIKR provide the essential services that underpin American society, whose exploitation or destruction could cause catastrophic health effects or mass casualties, or profoundly affect our national prestige and morale."[7] Additionally, HSPD-7 assigns the Department of Homeland Security (DHS) as lead agency for CIKR protection,[8] further breaks down CIKR into 18 sectors, and

assigns Sector Specific Agencies (SSA) to implement the National Infrastructure Protection Plan (NIPP).[9] Building on the requirements of HSPD-7, the DHS, in coordination with the DoD, published the NIPP, which assigned the DoD as the SSA charged with leading the effort to improve risk management of CIKR within the Defense Industrial Base (DIB).[10] Located within the DIB are 10 sectors, including the GIG sector, which is described as:

> *The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting…and managing on demand to warfighters, policy makers, and support personnel. It [GIG] includes all owned and leased communications (commercial telecommunications infrastructure) and computing systems and services, software, data, security services, and other associated services necessary to achieve information superiority.*[11]

Though the Homeland Security Act and NDAA have acted to increase cybersecurity, tomes of academic studies, along with congressional hearings, have uncovered a greater need for better synchronization of government agencies to apply a whole-of-government interagency approach to the challenge of defending the U.S. from a crippling cyber attack on CIKR and maintaining control of the GIG while conducting military operations in support of national objectives. U.S. military leaders, although not responsible for regulatory reform, are responsible for planning, developing, and resourcing capabilities for timely execution of cyberspace operations conducted in an interagency environment. The operational commander and the security of the U.S. are negatively impacted in the absence of legislation that provides firm performance standards to the private sector to defend CIKR and the GIG against cyber threats. U.S. Congress has conveyed concern that the lack of cyber security performance standards on American industry is similar to airlines operating without implementing the highest standards of safety and reliability.[12] Without regulations that establish a vigorous maintenance program for an airline, one could conclude a plane may crash from something that could have easily been

prevented. A comparison can be drawn between the aforementioned example given by the U.S. Congress and a cyber attack on industry that results in the failure of an electrical grid that could have been mitigated by more effective regulatory control of cybersecurity standards.

The Department of Defense's (DoD) participation within an interagency effort to develop partnerships with American industry is paramount to the cyber defense of the nation. Joint Publication (JP) 3-28, *Civil Support*, describes DoD as the supporting agency, providing Civil Support (CS) as directed by the President or Secretary of Defense (SecDef).[13] CS, otherwise known as Defense Support of Civil Authorities (DSCA), is defined by *JP 1-02* as:

> *Support provided by US Federal military forces…in response to requests for assistance from civil authorities for domestic emergencies, law enforcement support, and other domestic activities, or from qualifying entities for special events.*[14]

Cyber-DSCA has the strongest application to the continental U.S., but can encompass worldwide operational activities. JP 3-27, *Homeland Defense*, describes the integration of DoD into this domestic framework with its capability to provide a "global active, layered defense-in-depth of the homeland."[15] This defense strategy best complements the synchronization of the whole-of-government approach to achieve an effect against an adversarial threat. DoD is not a domestic Law Enforcement (LE) agency, which conducts an investigation to pursue the prosecution of nefarious subjects conducting cyber attacks against the U.S. Instead, the DoD employs this active, layered defense-in-depth to CIKR and the GIG and seeks to create an immediate operational effect, utilizing various methods to change the behavior of those nefarious state or non-state leaders, networks, and machine consoles.

The interagency cooperative effort, coupled with the statutory authorities governing DoD operational elements, poses challenges to the process of synchronizing Cyber-DSCA operations and protection of the GIG. The DoD is responsible for the protection of the GIG, as General

Keith Alexander, USA, commander, U.S. Cyber Command (USCYBERCOM), has asserted that his "first duty is to ensure that DoD networks are secure since securing these networks is crucial to protecting our data, to our warfighting potential, and ultimately to the defense of the nation."[16] These networks communicate critical information to the warfighting functions and components, and are crucial to the U.S. military's ability to develop forces, synchronize operational level logistic support to named operations, and execute full spectrum military operations through all operational phases. Challenges arise in defending these system networks because most are owned and operated by private sector entities and are not under DoD operational control. Given this, DoD is challenged with what it can or should be providing to other U.S. government agencies and key operators within the private sector to detect, deter, prevent, and thwart exploitation of U.S. CIKR and the GIG. USCYBERCOM brings immense capabilities to this collaborative effort and is facing a critical time to array and precisely employ forces to obtain control of the cyber domain, and to fight and win against all adversaries in a future cyber conflict. To address this challenge, these capabilities should carefully be mission managed to support interagency partners in the protection of CIKR, where unity of effort is the best strategy to precisely employ forces. Furthermore, USCYBERCOM's formal establishment of a Standing Joint Task Force-Cyber (SJTF-Cyber) in support of Cyber-DSCA and the "integration of National Guard (NG) and Reserve component forces"[17] will further balance the resourcing of these complex Cyber-DSCA operations.

Perspectives on Governing the Cyber Domain

The U.S. and many other state actors, such as Russia and China, are diametrically opposed in the methods of approaching the governance and defense of the cyber domain. The majority of U.S. critical infrastructure assets, Internet Service Providers, and telecommunications companies are privately owned and operated, and are consulted by the U.S. government to

coordinate improvements to the cyber security of critical infrastructure.[18] The U.S. government's policy on cyberspace results in creating the conditions where the private sector, as the end user, has the most influence to affect commerce and exercise free trade. The principle of this policy perspective is best presented in the *U.S. International Strategy for Cyberspace* where a collaborative world is described:

> *The U.S. will work to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation.*[19]

In contrast to the collaborative environment of U.S. cyberspace, China and many other nations, remain unalterably opposed to the U.S. policy of promoting a systems infrastructure that has limited regulation and oversight. The well-known Chinese Internet firewall, along with heavy regulations of industry, allows the Chinese government to restrict Internet freedoms to its vast population. Unlike the U.S. government's policy of leveraging partnerships with industry to protect infrastructure, the systems infrastructure in China is, for the most part, a state controlled enterprise.

The opposing perspectives of governance of the cyber domain were recently highlighted during the World Conference on International Telecommunications 2012 (WCIT-12). WCIT-12 is chaired by the Internet Telecommunications Union, which serves as the United Nations specialized agency for information and communications technology.[20] Min Jiang, a professor at University of North Carolina, suggests that WCIT-12 "openly highlighted the conflict dubbed the "digital cold war" between the U.S. "Internet freedom" agenda and the Sino-Russian vision of "Internet Sovereignty" which favors the authority of a highly restrictive nation."[21] During WCIT-12, a majority bloc of the nations in attendance, including China, Russia, and Iran, voted in favor of a resolution to allow governments new powers to heavily restrict Internet services.[22]

Cyber Threat to CIKR and the GIG

The domain of cyber warfare presents the most complex of challenges for the operational commander conducting operations in support of Cyber-DSCA or defense of the GIG. Without a restriction on operational space, an adversarial threat redefines, if not completely renders obsolete, the traditional positional advantages of operating from interior versus exterior lines of operations. Military theorist, Milan Vego, argues that cyberspace "blurs the boundaries of the theater, which increasingly becomes further complex and non-linear."[23] Vego further suggests that the operational factor of time is actively exploited by the threats, which are not constrained by international law,[24] to attack the decentralized systems of the U.S. CIKR or insert attack code into the GIG to prevent communications to the war fighter. Unlike other domains, there are no "down days" in conducting cyberspace operations as it can be argued that the cyber domain experiences no peacetime and cyber control is contested at all times. Additionally, cyberspace disruptions come at a minimal cost to an adversary resourcing operational activities. The *Quadrennial Homeland Security Review Report* describes the threat:

> *Sophisticated cyber criminals and nation-states…now pose great cost and risk both to our economy and national security. They exploit vulnerabilities in cyberspace to steal money and information, and to destroy, or threaten the delivery of critical services.*[25]

The need to protect critical services was recently highlighted when NSS Labs, Incorporated, published a report in 2011 identifying vulnerabilities within information control systems and Supervisory Control and Data Acquisition (SCADA) system applications created by the Beijing-based Sunway Force Control Technology Company.[26] The National Communications System identifies SCADA systems as applications that are used to monitor and control plants and equipment in a multitude of industries such as "telecommunications and energy, water and waste control, energy, oil and gas refining, and transportation."[27] Following

this report, the DHS issued an advisory explaining that these vulnerabilities could allow an attacker to perform a remote denial-of-service attack against the Sunway SCADA applications.[28] Although these vulnerabilities were evaluated and subsequently remedied, it is important to note that a number of U.S. companies, along with U.S. Allied countries, operate using SCADA applications developed by Chinese companies.[29] A denial-of-service attack on the SCADA system of a U.S. utility such as the electrical grid could have a disastrous effect if timed correctly during unsound environmental conditions or focused at critical locations.

The U.S. economy greatly depends on the operation of critical infrastructure and the uninhibited flow of information to facilitate commerce. This open commerce ultimately leads to American prosperity. Naval strategist, Geoffrey Till, describes how shipping is part of a "complex inter-modal goods distribution system involving ports, railways, and roads in which the essential unit is increasingly the container being transported by a variety of means."[30] Till goes on to describe an adversarial threat launching a cyber attack against the computerized logistics system of a shipping company, rather than seeking to threaten an individual container ship's port passage.[31] The analyses of these observations indicate that future adversaries, conducting cyberspace operations, may be able to achieve operational objectives by contesting sea control via the cyber domain and by obtaining temporary cyber control in the operational area. As a result, commanders must now encourage operational planners to allocate a substantial amount of time to analyzing the effect of the cyber environment on operational activities.

Vulnerabilities have also been identified in the GIG, which is already under cyber attack. Deputy Secretary of Defense William Lynn stated, " Our defense networks are probed thousands of times each day; they are scanned millions of times each day, and the frequency and the sophistication of those attacks are increasing exponentially."[32] This "probing" of networks

allows the adversarial threat a clear view into how DoD connects weapon platforms to their associated networks, or worse, how to disable that platform's network to shape the battlefield prior to conducting operational activities. In a recent step backwards on securing the GIG, the Pentagon, who has limited satellite bandwidth, recently announced its leasing of additional bandwidth on a Chinese, state-controlled satellite.[33] Noah Schactman from *Wired* suggests this relationship is dangerous, giving the Chinese insight into U.S. encryption capabilities and delivering to them the ability to deny access to the U.S. military's communication infrastructure.[34]

State and non-state adversarial threats are difficult to detect, and actors may use non-attributable means to project a protective guise to conceal cyberspace operational activities. The threat may use cheap, yet sophisticated, anonymizer software[35] to create a defense layer between themselves and the targeted CIKR asset or the GIG. Cyber adversaries target a multitude of American companies and just about every facet of American commerce and infrastructure."[36] The adversarial threat most notably proves its mettle by not only employing denial-of-service attacks, but by conducting a persistent cyber espionage campaign. China's Peoples Liberation Army, Unit 61398, has been exclusively branded as the primary unit targeting the U.S., aggressively collecting on economic and military related-intelligence.[37] Unit 61398, as reported in a recent due diligence study conducted by *Mandiant*, is responsible for the data theft of hundreds of terabytes of information ranging from satellites and telecommunications to the U.S. financial sector.[38]

Federal Agencies Responsible for Cyber Defense

General Alexander asserted, "We [DoD] do play a vital role in all of this, and in protecting DoD networks, supporting our combatant commanders, and defending the nation from

cyber attack, but we can't do it all. No agency here can do it all, as we have to have government and industry working together as a team."[39] Cyber homeland security is fundamentally an interagency effort and the interagency team is the fulcrum for the DoD's capability to provide forces to Cyber-DSCA. DoD serves as the federal department with lead responsibility for Homeland Defense (HD), and provides Cyber-DSCA in support of the DHS, who is designated as the lead agency for Homeland Security.[40] Nevertheless, immense challenges with coordination and information sharing arise when responding to attacks in a man-made domain, which digitally converges with all other domains of war fighting. The overarching construct of the cyber domain affects the private sector, all federal agencies, and every state and local government. Solving the challenges of protecting the U.S. homeland begins with bringing all of the aforementioned groups together in a collaborative information-sharing environment to protect the nation against cyber threats. The DHS is responsible for guiding this collaborative environment in what is known as the Cyber Unified Coordination Group (UCG) consisting of representatives from commercial industry, state and local governments, and various federal agencies.[41]

The ubiquitous character of cyberspace forces the DoD and other federal agencies to adapt to the realities of interagency coordination. If one was to look at the historical evolution of cyber interagency coordination on the scale of time it would reflect 1977 to 1988 as the dark ages; 1988 to 1996 as the middle ages; 1996 to 2010 as the age of enlightenment; and 2010 to present day as the modern era. DoD's transition to this modern era began in 2010 with the establishment of USCYBERCOM, a subordinate unified Command of U.S. Strategic Command (USSTRATCOM), which became DoD's focal point for conducting cyberspace operations. Undoubtedly, the convergence of DoD's existing cyber capabilities under USCYBERCOM

indicates the DoD is serious about conducting cyberspace operations and aligning DoD's efforts to better interagency coordination. As described in its mission statement, USCYBERCOM is "responsible for planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the DoD information networks and when directed, conduct full-spectrum military cyberspace operations in order to ensure U.S. and allied freedom of action in cyberspace, while denying the same to our adversaries."[42] Only if directed by the President or SecDef,[43] USCYBERCOM may be required to bring its immense capabilities to conduct Cyber-DSCA in the preparation for or during a sustained cyber attack against CIKR or the GIG. The National Response Framework (NRF) outlines a tiered process in which incidents are generally handled at the lowest jurisdictional level and provides a process for a state governor to request assistance from the President prior to DoD involvement.[44]

U.S. Northern Command (USNORTHCOM), U.S. Southern Command, and U.S. Pacific Command all synchronize, plan, and execute CS missions within the domestic portion of their respective Area Of Responsibility (AOR).[45] These Geographic Combatant Command's (GCC), with USSTRATCOM as the supporting command, are responsible for establishing an operational level framework to respond to natural disasters, pandemics, terrorism, ballistic missiles, chemical, biological, radiological, and nuclear attacks on the U.S. homeland.[46] USNORTHCOM serves as the Combatant Command (COCOM) for Standing Joint Task Force-CS (SJTF-CS), which is an operational level command that consists of active duty, NG, and Reserve component personnel from all service branches who are commanded by a federalized NG Officer to provide DSCA to the designated lead agency.[47] In the wake of a hypothetical cyber attack affecting the power grids of multiple U.S. cities, USNORTHCOM's SJTF-CS, if directed to support the lead agency, would be responsible for responding to the physical effects of the cyber attack. This

USNORTHCOM SJTF-CS model is suitable for USCYBERCOM to apply to its effective utilization of active, NG, and Reserve component forces and may be flexibly task organized into multiple rapid response packages to respond to a future cyber conflict.

Dealing with the complexity of cyberspace requires various responses to the threat and unity of effort in deciding what outcome best serves the interests of the nation. In March 2012, administration officials, along with the Chairman of the Joint Chiefs of Staff, attempted to strengthen support for improved procedures in the protection of CIKR by demonstrating to members of Congress what could happen if a cyber attack shut down the New York City electrical grid during a hot summer day.[48] This scenario serves to paint a frightening picture of what a major U.S. city would experience during a persistent denial-of-service attack lasting one week or longer. Medical life-support systems would fail and a devastating impact to the economy would occur with the closure of the New York Stock Exchange, undoubtedly requiring a response from the President or SecDef. In the fictional scenario above, USCYBERCOM, in coordination with the National Security Agency (NSA), could attribute the attack to a specific threat through cyber due diligence and conduct a retaliatory network attack, or USSTRATCOM could provide the option to apply a kinetic strike response. As part of the UCG collaborative environment, other options from entities such as DHS, the Federal Bureau of Investigation (FBI), state law enforcement or local authorities, or a states NG may also be provided for consideration in the President's decision making process.

JP 3-28, *Civil Support*, describes HD and DSCA missions as separate and distinct, but some departments have roles and responsibilities that overlap, and the lead and supporting roles may transition rapidly between organizations.[49] This collaborative effort's synchronization is also challenged by other organizations conducting additional operations in response to the same

cyber attack. Similarities can be drawn between the challenges associated with cyber attack response plans and the Maritime Operations Threat Response (MOTR) process. Research conducted by the U.S. Naval War College regarding which government agency would respond or lead the MOTR effort, may best be summed up with the comment, "it depends."[50] The study describes the concerted effort in responding to a threat that can be governed by the following considerations: advantage to the nation, legal authorities, agency capacity, and capabilities readily available to preempt or counter the threat.[51] The flexible nature of a response plan that counters a cyber threat addresses many of the same considerations as the MOTR process and provides for greater alternatives than a "one size fits all" threat response. These alternatives can provide for a whole-of government approach ranging from doing nothing to conducting a LE investigation, or conducting a B-2 Bomber strike. As noted above, the response "depends" on what is most profitable to the nation and what capabilities exist against the threat.

USCYBERCOM, operating under Title 10 authorities (Computer Defense/Attack), in coordination with the National Security Agency (NSA), operating under Title 50 authorities (Computer Exploitation/Collection), provides immense capabilities to interagency partners to properly identify the cyber adversary, submit intervention plans, or conduct operational activities against adversaries that present an imminent danger to the U.S.[52] However, USCYBERCOM's precise targeting process and neutralization of specific adversaries may not be the optimal choice for the President or SecDef in some cases. Other desired end states may include the investigation and subsequent prosecution of subjects conducting cybercrime or cyberterrorism. The Federal Bureau of Investigation (FBI), operating under Title 18 authorities, is the lead LE agency for investigating subjects who conduct domestic cyber attacks.[53] USCYBERCOM may be able to send attack code to systematically dismantle a foreign adversary's capabilities, and

while this method degrades the adversary's capabilities, it may eliminate any possibility the FBI had to develop a case for prosecution. Again, "it depends."

DOD Support to DHS and the DIB

DHS serves as the lead agency and national focal point for cyber incident management and coordination during cyber incidents. The National Cyber Incident Response Plan (NCIPR) was developed according to the principles presented in the NRF and describes how the Nation responds to Significant Cyber Incidents (SCI) such as the fictional cyber attack scenario on the New York City electrical grid previously described.[54] The NCIPR is a guide that provides a wide-ranging collaborative structure for responding to an attack that is underway or the attacker that maintains persistence in future attacks against similar targeted platforms. DHS's National Cybersecurity and Communications Integration Center (NCCIC), serves as the entity providing the "central point of coordination for national response efforts and activities regarding significant cyber incidents."[55]

The NCCIC operates in two primary phases: steady-state response and SCI response. During steady-state operations, the NCCIC actively works with industry owners of CIKR, whether private sector or state-owned to enhance their cyber security preparedness, risk assessment and incident response capabilities.[56] When a SCI occurs, the NCCIC convenes the Cyber UCG Incident Management Team (UCG IMT). The Cyber UCG IMT as described in the NCIPR as a group, "which always includes a senior defense representative, is a pool of senior officials and staff that represent their department or organization and able to quickly describe their organizations capacity and commit their organizations resources to assist in the SCI response."[57] This interagency composition is important because most SCI responses transcend the authorities, capabilities, and capacity of a single organization. Following the SCI, the

NCCIC concept of the operations outlines that the Cyber UCG IMT is responsible for the following: "establishing the incident action plan; ensuring overall coordination of SCI management and resource activities; facilitating interagency conflict resolution; coordinating response when multiple cyber events occur; and ensuring that the National Operations Center receives timely updates on response activities."[58]

The NCCIC and the DoD work in close collaboration during the steady-state and SCIs and share personnel through cross-assignment as outlined in a Memorandum of Agreement (MOA) between DoD and DHS.[59] This MOA was subsequently codified into law in the NDAA of 2012.[60] Prior to 2012, a wise leader would have seen this MOA passed into law as necessary, given the numerous accounts of failures in information sharing amongst government agencies. Nevertheless, under this MOA, the NSA integrates DHS personnel into its NSA/Central Security Service Threat Operations Center (NTOC) and the Joint Coordination Element for "joint operational planning and synchronization in order to promote DHS mission support for HS for cybersecurity."[61] DHS, as outlined in the MOA, also integrates an NSA Cryptologic Services Group and a USCYBERCOM Cyber Support Element into the NCCIC for operational synchronization with the NCIRP.[62] This MOA was the forcing function to formalize the synchronization between DHS and USCYBERCOM operational elements and bridge gaps with information sharing. Although information-sharing challenges remain, the knitting together of DHS and DoD operational elements must be materialized and maintained with other agencies as well. To address these challenges, the aforementioned MOA provides a model for maintaining a persistent physical presence of integrated analysts and liaison officers within all corresponding interagency cells. This physical presence, vice a virtual presence, develops relationships and builds trust in a critical time where unity of effort is the best, if not the only, strategy to precisely

employ forces.

The challenge still remains with increasing dialogue and information sharing with the private sector to identify cyber threat signatures, while being cognizant of protecting the civil liberties of U.S. citizens.[63] The result of these challenges going unaddressed will be to leave DHS and DoD blind to ongoing cyber attacks and reliant on the private sector being responsible for reporting the attacks. The NDAA of Fiscal Year 2013, made great strides with levying reporting requirements over "cleared defense contractors," which includes a large portion of the DIB and all private sector entities granted security clearances.[64] General Alexander correctly stated, "I think that's [NDAA 2013] a step in the right direction, but the issue would be with the DIB, as they don't see all the threats coming in all the time and oftentimes the threats that we see has gotten in [DIB systems] long before. I think we need a total approach."[65]

DoD Directive 3020.40 establishes that USCYBERCOM, in coordination with the Defense Information Systems Agency, who is the defense infrastructure lead agency for the GIG, collaborates with DIB asset owners and operators to strengthen the security of their networks through a layered defense approach similar to the NRF.[66] The main intent of the DIB sector specific plan, developed in coordination with industry owners of CIKR, is to deter cyber threats to DIB assets. These sector specific plans ultimately tie directly into the NIPP, and the DoD, as SSA lead for the DIB, provides input to the Cyber UCG when needed during steady-state operations or SCI responses. The DoD sector specific plan applies the following guidelines when providing an active defense to DIB CIKR: "First Level: Asset owners responsible; Second Level: As threat escalates, local authorities assist asset owners in protection responsibilities; Third Level: State and Federal LE authorities augment local authorities; Fourth Level: State Governor may request other Federal assistance or employ NG (Title 32 Authorities) under his

command and control; and Fifth Level: President employs U.S. military (USCYBERCOM Cyber Counter Strike) forces to protect DIB assets."[67] These types of guidelines on response may be applied to other SSA's in the U.S. Government such as banking and finance or energy.

In March 2013, USCYBERCOM announced plans to field capabilities to conduct three missions: "defend the nation from attack; support the GCC's; and defend DoD networks."[68] USCYBERCOM's Service Components have hurried the process for actively developing and training this capacity to effectively meet the aforementioned mission sets. In a groundbreaking step forward, USCYBERCOM announced the future establishment of cyber teams aligned against the aforementioned mission sets. This USCYBERCOM initiative is developing the following forces to array against cyber threats: "a Cyber National Mission Force to defend the nation; a Cyber Combat Mission Force assigned to the Operational Control (OPCON) of individual GCC's; and a Cyber Protection Force to help operate and defend the DoD information environment."[69]

Recommendations and Conclusion

The current operational challenges in cyber homeland defense facing the DoD are accomplishing the rapid growth necessary to support the expansion of cyber forces and determining how USCYBERCOM will effectively mission manage their operational activities. The cyber units mentioned above should be mission managed in a manner that best facilitates USCYBERCOM's ability to effectively respond to threats worldwide. It is well known that the character of cyberspace operational activities transcends the geographic boundaries of the U.S. and the respective GCC's AOR. Therefore, it is imperative that USCYBERCOM maintain COCOM and resourcing over all cyber units while continuing to serve in a supporting role to the GCC's for all cyber activities conducted in their respective AOR's. In David Hathaway's, "*The*

Digital Kasserine Pass," it is suggested that USCYBERCOM maintain COCOM and be capable of transferring cyber forces to other AOR's in support of other contingent operations.[70]

USNORTHCOM's SJTF-CS provides a tested model[71] on which to lay a foundation for establishing a USCYBERCOM SJTF-Cyber responsible for Cyber-DSCA. Under this model, USCYBERCOM, in coordination with USNORTHCOM, would exercise COCOM over the SJTF-Cyber Headquarters and select a Service Component to develop and lead this operational level organization. An operational SJTF-Cyber Headquarters, operating under a general officer, provides the USCYBERCOM Commander with a full time organization that is operationally focused on instantaneous SCI response in support of Cyber-DSCA. Additionally, the SJTF-Cyber, not unlike USNORTHCOM's SJTF-CS, would provide DSCA support to the lead federal agency, exponentially increase Reserve Component Forces into the framework, and be capable of operating in multiple Joint Operational Areas. The resourcing of this SJTF-Cyber is challenged by the current limited capacity of USCYBERCOM. Similar to USNORTHCOM, USCYBERCOM should "mitigate this limited capacity with Reserve Component augmentation"[72] of the SJTF-Cyber. Operational planners at USCYBERCOM should be able to design force structure models that are easily modified for responding to various SCIs.

USCYBERCOM profits by maintaining an effort to assist in the development of NG forces and incorporate Reserve component forces in its framework to conduct Cyber-DSCA. In order to address the challenge of reducing the strain on the services and better array force capabilities to conduct Cyber-DSCA, the NG and Reserve components should be made more available to exponentially increase capacity to USCYBERCOM.[73] The U.S. Army's Cyberspace Concept Capability Plan describes NG and Reserve personnel as well versed in technical fields and can be utilized to increase capacity.[74] This plan also suggests that NG and Reserve

Components are better suited to recruit highly skilled Soldiers that are already working in the civilian industry.[75] In research conducted by the Air University, an argument was aptly made for the creation of a "NG Cybersecurity Program that integrates forces, operating in a Title 32 status, into DHS's NCCIC, NSA's NTOC, the FBI, and integrates additional forces into USCYBERCOM."[76] These additional forces serving in this capacity may better free up other USCYBERCOM operational elements and provide for an absolute force strategy that is more conducive to protecting against cyber threats to CIKR that are evolutionary and global.

Appendix A

List of Acronyms

AOR	Area of Responsibility
CIKR	Critical Infrastructure and Key Resources
COCOM	Combatant Command
CS	Civil Support
DSCA	Defense Support of Civil Authorities
DIB	Defense Industrial Base
DHS	Department of Homeland Security
DOD	Department of Defense
FBI	Federal Bureau of Investigation
GCC	Geographic Combatant Command
GIG	Global Information Grid
HD	Homeland Defense
IMT	Incident Management Team
HSPD	Homeland Security Presidential Directive
JP	Joint Publication
LE	Law Enforcement
MOA	Memorandum of Agreement
MOTR	Maritime Operations Threat Response
NCCIC	National Cybersecurity and Communications Integration Center
NCIPR	National Cyber Incident Response Plan
NDAA	National Defense Authorization Act
NG	National Guard
NIPP	National Infrastructure Protection Plan
NRF	National Response Framework
NSA	National Security Agency
NTOC	National Security Agency Threat Operation Center
OPCON	Operational Control
SCI	Significant Cyber Incident
SCADA	Supervisory Control and Data Acquisition
SECDEF	Secretary of Defense
SSA	Sector Specific Agency
SJTF	Standing Joint Task Force
UCG	Unified Coordination Group
USCYBERCOM	U.S. Cyber Command
USNORTHCOM	U.S. Northern Command
USSTRATCOM	U.S. Strategic Command
WCIT	World Conference on International Telecommunications

Notes

[1] President Barrack Obama. Executive Order. "Improving Critical Infrastructure Cybersecurity." Section 1, Policy (Washington, DC: White House, 12 February 2013).
[2] Scott Brown, "*WarGames*: A Look Back at the Film That Turned Geeks and Phreaks Into Stars," *Wired.com*, 21 July 2008. accessed 10 April 2013, http://www.wired.com/entertainment/hollywood/magazine/16-08/ff_war games?currentPage=all.
[3] Compilation, "Timeline: The U.S. Government and Cybersecurity," *Washingtonpost.com*, 16 May 2003, accessed on 4 April 2013, http://www.washingtonpost.com/wp-dyn/articles/ A50606-2002Jun26.html.
[4] *The Computer Security Act of 1987*, U.S. Statutes (1987): 40 USC sec. 2.
[5] *Homeland Security Act of 2002*, Public Law 107-296, 107th Cong., *Public Law*, (25 November 2002): sec. 225.
[6] *National Defense Authorization Act for Fiscal Year 2012*, HR 1540, 112th Cong., *Congressional Record*, (31 December 2011): sec 1090.
[7] President George W. Bush, Homeland Security Presidential Directive-7, "Critical Infrastructure Identification, Prioritization, and Protection," sec. 4 (Washington, DC: White House, 17 December 2003).
[8] Ibid., sec. 12.
[9] U.S. Department of Homeland Security, *National Infrastructure Protection Plan: Partnering to enhance protection and resiliency* (Washington, DC: Office of the Secretary of Homeland Security, 2009), 2-3.
[10] U.S. Department of Defense, *Defense Industrial Base: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Plan* (Washington, DC: Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, May 2007), 3.
[11] U.S. Department of Defense, DoD Policy and Responsibility for Critical Infrastructure, Department of Defense Directive (DODD) 3020.40 (Washington DC: DoD, 21 September 2012), 16.
[12] Hank Johnson, "Testimony," House, *What Should the Department of Defenses Role in Cyber Be: Hearing before the Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services*, 112th Cong., 1st Sess., 2011, 15.
[13] Chairman, U.S. Joint Chiefs of Staff (CJCS), *Civil Support*, Joint Publication (JP) 3-28 (Washington, DC: CJCS, 14 September 2007), I-5-I-6.
[14] Chairman, U.S. Joint Chiefs of Staff (CJCS), *Department of Defense Dictionary of Military and Associated Terms*. as amended, Joint Publication 1-02 (Washington, DC: CJCS, 15 March 2013), 77.
[15] Chairman, U.S. Joint Chiefs of Staff (CJCS), *Homeland Defense*, Joint Publication 3-27 (Washington, DC: CJCS, 12 July 2007), I-5.
[16] General Keith Alexander, "Opening Statement," House, *Fiscal Year 2012 Budget Request from U.S. Cyber Command: Hearing before the Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services*, 112th Cong., 1st Sess., 10.
[17] Maurice M. McKinney, *A National Solution: Rethinking The Employment of Air National Guard Title 32 Status Citizen-Airmen To Defend The Nations Cyberspace* (Maxwell AFB, AL: Air University, 2013), 2, accessed 25 April 2013, http://www.au.af.mil/au/awc/awcgate/awc/ mckinney.pdf.
[18] President Barrack Obama. Executive Order. "Improving Critical Infrastructure Cybersecurity." Section 6, Policy (Washington, DC: White House, 12 February 2013).
[19] President Barrack Obama. *The International strategy for Cyberspace* (Washington, DC: White House, May 2011). 8.
[20] The International Telecommunications Union (ITU). "Overview," ITU Webpage, accessed 10 May 2013, http://www.itu.int/en/about/Pages/overview.aspx.
[21] Min Jiang, "China's "Internet Sovereignty" in the Wake of WCIT-12," *China U.S. Focus*, 6 February 2013. Accessed on 9 May 2010, http://www.chinausfocus.com/peace-security/chinas-internet-sovereignty-in-the-wake-of-wcit-12/.
[22] L. Gordon Crovitz, "America's First Big Digital Defeat," *Wallstreetjounal.com*, 16 December 2012. Accessed on 10 May 2013, http://online.wsj.com/article/SB10001424127887323981504 5781815 33577508260.html.
[23] Milan N. Vego, *Joint Operational Warfare: Theory and Practice*, (2007; repr., U.S. Naval War College, 2009), XIV-8.
[24] Ibid.
[25] U.S. Department of Homeland Security, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland* (Washington, DC: Office of the Secretary of Homeland Security, February 2010), 29.

[26] Jeremy Kirk, "U.S. warns of problems in Chinese SCADA software," *CIO.com*, 17 June 2011, http://www.cio.com.au/article/390584/us_warns_problems_chinese_scada_software/.
[27] Office of the Manager of National Communications System, *Technical Information Bulletin 04-01: Supervisory Control and Data Acquisitions Systems*," (October 2004): 4.
[28] U.S. Department of Homeland Security, "Alert (ICS-Alert-11-238-01A): Sunway Force Control SCADA SHE 6.1 (Update A). *DHS.gov*, accessed 10 May 2013, http://ics-cert.us-cert.gov/alerts/ICS-ALERT-11-238-01A.
[29] Wei Tian, "Software Bugs Discovered In Chinese Made Applications," *ChinaDaily.com*, 18 June 2011. Accessed 13 May 2013, http://www.chinadaily.com.cn/cndy/2011-06/18/content_ 12727638.htm.
[30] Geoffrey Till, "A Changing Focus for the Protection of Shipping" in the Strategic Importance of Seaborne Trade and Shipping: A Common Interest of Asia Pacific, ed. Forbes, Andrew. Canberra, Australia: Sea Power Centre – Australia, 2002. (NWC 4032).
[31] Ibid.
[32] Sean Lawson, "Just How Big Is The Cyber Threat to The Department Of Defense," *Forbes.com*, 04 June 2010. Accessed on 24 April 2013, http://www.forbes.com/sites/firewall/2010/06/04/just-how-big-is-the-cyber-threat-to-dod/.
[33] Douglas L. Loverro, "Testimony," House, *Fiscal Year 2014 National Defense Authorization Budget Request for National Security Space Activities: Hearing before the Subcommittee on Strategic Forces of the Committee on Armed Services*, 112th Cong., 1st Sess.

[34] Noah Scachtman, "Pentagon Paying China-Yes, China-To Carry Data," *Wired.com*, 29 April 2013. Accessed on 5 May 2013, http://www.wired.com/dangerroom/2013/04/china-pentagon-satellite/.
[35] Anonymizer Universal, Trademarked, "How It Works," *Anonymizer.com*. Accessed on 13 May 2013, https://www.anonymizer.com/homeuser/universal/index.php#howitworks.
[36] David Fieth, "Timothy Thomas: Why China Is Reading Your Email," *Wallstreetjournal.com*. Accessed on 5 May 2013, http://online.wsj.com/article/SB100 01424127887323419104578376 042379430724.html.
[37] Mark A. Stokes, Jenny Lin, and L.C. Russell Hsiao, *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure* (Project 2049 Institute: 11 November 2011), 8.

[38] MANDIANT, "APT 1: "Exposing One of China's Cyber Espionage Units," accessed 04 May 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.
[39] Tyrone C. Marshall Jr. SFC, USA, "Cybercom Commander Calls Cybersecurity Order First Step," *Armed Forces Press Service*, 13 February 2013. Accessed on 3 May 2013, http://www.defense.gov/news/newsarticle.aspx ?id= 119286.
[40] Chairman, U.S. Joint Chiefs of Staff (CJCS), Civil Support. as Joint Publication 3-28 (Washington, DC: CJCS, 14 September 2007), vii.
[41] U.S. Department of Homeland Security, *National Cyber Incident Response Plan: Interim Version* (Washington, DC: Office of the Secretary of Homeland Security, September 2010), v.
[42] U.S. Strategic Command Official Website, "U.S. Cyber Command," accessed 04 May 2013, http://www.stratcom.mil/factsheets/Cyber_Command/.
[43] U.S. Department of Homeland Security, *National Response Framework* (Washington, DC: Office of the Secretary of Homeland Security, January 2008), 26.
[44] Ibid.
[45] Chairman, U.S. Joint Chiefs of Staff (CJCS), *Civil Support*, Joint Publication (JP) 3-28 (Washington, DC: CJCS, 14 September 2007), II-9-10.
[46] Ibid., I-5-I-6.
[47] U.S. Northern Command Website, "Joint Task Force Civil Support Fact Sheet," accessed 13 May 2013, http://www.jtfcs.northcom.mil/JTFCS.aspx.
[48] Michael S. Schmidt, "Senators Force Weaker Safeguards Against Cyberattacks," *NewYorkTimes.com*, 27 July2012. Accessed on 06 May 2013, http://www.nytimes.com/2012/07/28/us/politics/new-revisions-weaken-senate-cybersecurity-bill.html?pagewanted=all&_r=1&.
[49] Chairman, U.S. Joint Chiefs of Staff (CJCS), Civil Support. as Joint Publication 3-28 (Washington, DC: CJCS, 14 September 2007), vii.
[50] Ivan T. Luke, *The Challenges of Maritime Homeland Security & Defense* (Newport, RI: U.S. Naval War College, 2013), 5, accessed 03 May 2013.

[51] Ibid.
[52] U.S. Department of Homeland Security, *National Cyber Incident Response Plan: Interim Version* (Washington, DC: Office of the Secretary of Homeland Security, September 2010), 9.
[53] The Federal Bureau of Investigation Website, "Frequently Asked Questions," accessed 13 May 2013, http://www.fbi.gov/about-us/faqs.
[54] U.S. Department of Homeland Security, *National Cyber Incident Response Plan: Interim Version* (Washington, DC: Office of the Secretary of Homeland Security, September 2010), v.
[55] U.S. Department of Homeland Security, *National Cybersecurity and Communications Integration Center: Concept of Operations, Version 3.7* (Washington, DC: Office of the Assistant Secretary for Cybersecurity and Communications, 3 May 2001), 6. For Official Use Only.
[56] U.S. Department of Homeland Security, "DHS Cybersecurity Mission and Capabilities" (PowerPoint presentation, no date provided). For Official Use Only.
[57] U.S. Department of Homeland Security, *National Cyber Incident Response Plan: Interim Version* (Washington, DC: Office of the Secretary of Homeland Security, September 2010), 14-15.
[58] U.S. Department of Homeland Security, *National Cybersecurity and Communications Integration Center: Concept of Operations, Version 3.7* (Washington, DC: Office of the Assistant Secretary for Cybersecurity and Communications, 3 May 2001), 19. For Official Use Only.
[59] Secretary of Defense to Secretary of Homeland Security. memorandum of agreement, 13 October 2010.
[60] *National Defense Authorization Act for Fiscal Year 2012*, HR 1540, 112th Cong., *Congressional Record*, (31 December 2011): sec 1090.
[61] Secretary of Defense to Secretary of Homeland Security. memorandum of agreement, 13 October 2010.
[62] Ibid.
[63] General Keith Alexander, "Testimony," Senate, *U.S. Strategic Command and U.S. Cyber Command in review of the Defense Authorization Request for Fiscal Year 2014 and the Future Years Defense Program*: *Hearing before the Committee on Armed Services*, 112th Cong., 1st Sess., 9.
[64] *National Defense Authorization Act for Fiscal Year 2013*, HR. 4310, 112th Cong., *Congressional Record*, (3 January 2012): sec 941.
[65] General Keith Alexander, "Testimony," Senate, *U.S. Strategic Command and U.S. Cyber Command in review of the Defense Authorization Request for Fiscal Year 2014 and the Future Years Defense Program*: *Hearing before the Committee on Armed Services*, 112th Cong., 1st Sess., 13.
[66] U.S. Department of Defense, DoD Policy and Responsibility for Critical Infrastructure, Department of Defense Directive (DODD) 3020.40 (Washington DC: DoD, 21 September 2012), 14.
[67] U.S. Department of Defense, *Defense Industrial Base: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Plan* (Washington, DC: Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, May 2007), 23.
[68] General Keith Alexander, "Testimony," Senate, *U.S. Strategic Command and U.S. Cyber Command in review of the Defense Authorization Request for Fiscal Year 2014 and the Future Years Defense Program*: *Hearing before the Committee on Armed Services*, 112th Cong., 1st Sess., 24.
[69] General Keith Alexander, "Opening Statement," House, *Information Technology and Cyber Operations: Modernization and Policy Issues to Support the Future Force: Hearing before the Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services*, 112th Cong., 1st Sess., 6-7.
[70] David C. Hathaway, *The Digital Kasserine Pass: The Battle Over Command and Control of DOD's Cyber Forces* (Maxwell AFB, AL: Air University, 2011), 18-19, accessed 14 May 2013, http://www.brookings.edu/~/media/research/files/papers/2011/7/15%20cyber%20forces%20hathaway/0715_cyber_forces_hathaway.pdf.
[71] U.S. Northern Command, "JTF-CS 101 Brief" (PowerPoint presentation, 29 November 2012). UNCLASSIFIED.
[72] Maurice M. McKinney, *A National Solution: Rethinking The Employment of Air National Guard Title 32 Status Citizen-Airmen To Defend The Nations Cyberspace* (Maxwell AFB, AL: Air University, 2013), 5, accessed 25 April
[73] Ibid., 2.
[74] U.S. Army, *Cyberspace Operations Concept Capability Plan 2016*-2028, TRADOC Pamphlet 525-7-8 (Fort Monroe, VA: Department of the Army, 22 February 2010), 33, accessed 10 May 2013, http://www.tradoc.army.mil/tpubs/pams/tp525-7-8.pdf.
[75] Ibid.

[76] Maurice M. McKinney, *A National Solution: Rethinking The Employment of Air National Guard Title 32 Status Citizen-Airmen To Defend The Nations Cyberspace* (Maxwell AFB, AL: Air University, 2013), 13, accessed 25 April 2013, http://www.au.af.mil/au/awc/awcgate/awc/ mckinney.pdf.

Bibliography

Andrues, Wesley R. "What Cyber Command Must Do." Joint Force Quarterly, no. 59, 2010. Accessed 9 April 2013. http://www.ndu.edu/press/what-US-cyber-command-must-do.html.

Anonymizer Universal, Trademarked. "How It Works." *Anonymizer.com*. Accessed on 13 May 2013. https://www.anonymizer.com/homeuser/universal/index.php#howitworks.

Barkley, Kevin Campbell, Joseph Roybal. *"Interagency Coordination @ Net Speed: Recommendations to Maximize Interagency Coordination and Capabilities At US CYBERCOM."* Harvard University: Kennedy School, 23 May 2010.

Brown, Scott. "WarGames: A Look Back at the Film That Turned Geeks and Phreaks Into Stars." *Wired.com*, 21 July 2008. Accessed 10 April 2013. http://www.wired.com/entertainment/hollywood/magazine/16-08/ff_wargames?currentPage=all.

Compilation. "Timeline: The U.S. Government and Cybersecurity." *Washingtonpost.com*, 16 May 2003. Accessed on 4 April 2013. http://www.washingtonpost.com/wp-dyn/articles/A50606-2002Jun26.html.

Computer Security Act of 1987. U.S. Statutes (1987): 40 USC.

Crovitz, L. Gordon. "America's First Big Digital Defeat." *Wallstreetjounal.com*, 16 December 2012. Accessed on 10 May 2013. http://online.wsj.com/article/SB10001424127887323915045 781815 33577508260.html.

Federal Bureau of Investigation. "Frequently Asked Questions." Accessed 13 May 2013. http://www.fbi.gov/about-us/faqs.

Fieth, David. "Timothy Thomas: Why China Is Reading Your Email." *Wallstreetjournal.com*. Accessed on 5 May 2013. http://online.wsj.com/article/SB10001424127887323419104578376 042379430724.html.

Hathaway, David C. *The Digital Kasserine Pass: The Battle Over Command and Control of DOD's Cyber Forces*. Maxwell AFB, AL: Air University, 2011. http://www.brookings.edu/~/media/research/files/papers/2011/7/15%20cyber%20forces%20hathaway/0715_cyber_forces_hathaway.pdf.

Homeland Security Act of 2002. U.S. Statutes (2002). sec. 225.

International Telecommunications Union. "Overview," ITU Webpage. Accessed 10 May 2013. http://www.itu.int/en/about/Pages/overview.aspx.

Jiang, Min. “China’s “Internet Sovereignty” in the Wake of WCIT-12.” *China U.S. Focus*, 6 February 2013. Accessed on 9 May 2013. http://www.chinausfocus.com/peace-security/chinas-internet-sovereignty-in-the-wake-of-wcit-12/.

Kirk, Jeremy Kirk. “U.S. warns of problems in Chinese SCADA software.” *CIO.com*, 17 June 2011. Accessed 20 April 2013. http://www.cio.com.au/article/390584/us_warns_problems_chinese_scada_software/.

Lawson, Sean. “Just How Big Is The Cyber Threat to The Department Of Defense.” *Forbes.com*. 04 June 2010. Accessed on 24 April 2013. http://www.forbes.com/sites/firewall/2010/06/04/just-how-big-is-the-cyber-threat-to-dod/.

Luke, Ivan T. *The Challenges of Maritime Homeland Security & Defense*. Newport, RI: U.S. Naval War College, 2013.

Mandiant. “APT 1: “Exposing One of China’s Cyber Espionage Units.” Accessed 04 May 2013. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

Marshall, Tyrone C., Jr, SFC, USA. “Cybercom Commander Calls Cybersecurity Order First Step.” *Armed Forces Press Service*, 13 February 2013. Accessed on 3 May 2013. http://www.defense.gov/news/newsarticle.aspx ?id=119286.

McKinney, Maurice M. *A National Solution: Rethinking The Employment of Air National Guard Title 32 Status Citizen-Airmen To Defend The Nations Cyberspace*. Maxwell AFB, AL: Air University, 2013. Accessed 10 May 2013. http://www.au.af.mil/au/awc/awcgate/awc/mckinney.pdf.

National Defense Authorization Act of 2012. U.S. Statutes (2012). sec. 951.

National Defense Authorization Act of 2013. HR 4310 (2012). sec, 941.

Office of the Manager of National Communications System. *Technical Information Bulletin 04-01: Supervisory Control and Data Acquisitions Systems*.” October 2004.

Reuters. “Aramco Says Cyber Attack Was Aimed at Production.” *New York Times*, 9 December 2012. Accessed 25 April 2013. http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html?_r=0.

Scachtman, Noah. “Pentagon Paying China-Yes, China-To Carry Data.” *Wired.com*. 29 April 2013. Accessed on 5 May 2013. http://www.wired.com/dangerroom/2013/04/china-pentagon-satellite/.

Schmidt Michael S. "Senators Force Weaker Safeguards Against Cyberattacks." *NewYorkTimes.com*. 27 July2012. Accessed on 06 May 2013. http://www.nytimes.com/2012/07/28/us/politics/new-revisions-weaken-senate-cybersecurity-bill.html?pagewanted=all&_r=1&.

Secretary of Defense. Secretary of Defense to Secretary of Homeland Security. Memorandum of agreement, 13 October 2010.

Stokes, Jenny Lin, and L.C. Russell Hsiao. *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*. Project 2049 Institute: 11 November 2011.

Till, Geoffrey. "A Changing Focus for the Protection of Shipping" in the Strategic Importance of Seaborne Trade and Shipping: A Common Interest of Asia Pacific, ed. Forbes, Andrew. Canberra, Australia: Sea Power Centre – Australia, 2002.

U.S. Army. *Cyberspace Operations Concept Capability Plan 2016*-2028. TRADOC Pamphlet 525-7-8. Fort Monroe, VA: Department of the Army, 22 February 2010.

U.S. Congress. House. *Fiscal Year 2012 Budget Request from U.S. Cyber Command: Hearing before the Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services*. 112th Cong., 1st Sess., 2011.

_____. House. *Fiscal Year 2014 National Defense Authorization Budget Request for National Security Space Activities: Hearing before the Subcommittee on Strategic Forces of the Committee on Armed Services*, 113th Cong., 1st Sess. 2013.

_____. House. *Information Technology and Cyber Operations: Modernization and Policy Issues to Support the Future Force: Hearing before the Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services*. 113th Cong., 1st Sess., 2013.

_____. House. *National Defense Authorization Act for Fiscal Year 2012*. HR 1540. 112th Cong., *Congressional Record*, (31 December 2011): sec. 1090.

_____. House. *What Should the Department of Defenses Role in Cyber Be: Hearing before the Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services*. 112th Cong., 1st sess., 2011.

_____. Senate. *U.S. Strategic Command and U.S. Cyber Command in review of the Defense Authorization Request for Fiscal Year 2014 and the Future Years Defense Program*: *Hearing before the Committee on Armed Services*.112th Cong., 1st Sess., 2013.

U.S. Department of Defense. *Defense Industrial Base: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Plan*. Washington, DC: DoD, May 2007.

_____. DoD Policy and Responsibility for Critical Infrastructure, Department of Defense Directive (DODD) 3020.40. Washington, DC: DoD, 21 September 2012.

_____. DoD Policy and Responsibility for Critical Infrastructure, Department of Defense Directive (DODD) 3020.40 (Washington DC: DoD, 21 September 2012), 14.

U.S. Department of Homeland Security. "Alert (ICS-Alert-11-238-01A): Sunway Force Control SCADA SHE 6.1 (Update A)." *DHS.gov*. Accessed 10 May 2013. http://ics-cert.us-cert.gov/alerts/ICS-ALERT-11-238-01A.

_____. "DHS Cybersecurity Mission and Capabilities." PowerPoint presentation, no date provided. DHS. For Official Use Only.

_____. *National Cyber Incident Response Plan: Interim Version*. Washington, DC: DHS September 2010.

_____. *National Cybersecurity and Communications Integration Center: Concept of Operations, Version 3.7*. Washington, DC: DHS, 3 May 2001. For Official Use Only.

_____. *National Infrastructure Protection Plan: Partnering to enhance protection and resiliency*. Washington, DC: DHS, 2009.

_____, *National Response Framework*. Washington, DC: DHS, January 2008.

_____. *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland*. Washington, DC: DHS, February 2010.

U.S. Northern Command. "JTF-CS 101 Brief." PowerPoint presentation, 29 November 2012.

_____. "Joint Task Force Civil Support Fact Sheet." Accessed 13 May 2013. http://www.jtfcs.northcom.mil/JTFCS.aspx.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Civil Support*. Joint Publication (JP) 3-28. Washington, DC: CJCS, 14 September 2007.

_____. *Department of Defense Dictionary of Military and Associated Terms*. As amended. Joint Publication 1-02. Washington, DC: CJCS, 15 March 2013.

_____. *Homeland Defense*. Joint Publication 3-27.Washington, DC: CJCS, 12 July 2007.

_____. *Information Operations*. Joint Publication 3-13. Washington, DC: CJCS, 27 November 2012.

_____. *Joint Task Force Headquarters*. Joint Publication 3-33, Washington, DC: CJCS, 30 July 2012.

U.S. President. Executive Order. “Improving Critical Infrastructure Cybersecurity.” sec. 1, Policy. Washington, DC: White House, 12 February 2013.

_____. Homeland Security Presidential Directive-7. *“Critical Infrastructure Identification, Prioritization, and Protection.”* sec. 4, 6. Washington, DC: White House, 17 December 2003.

_____. *International Strategy for Cyberspace*. Washington, DC: White House, May 2011.

_____. *National Strategy for Information Sharing and Safeguarding*. Washington, DC: December 2012.

_____. *The Comprehensive National Cybersecurity Strategy Initiative*. Washington DC: White House, March 2010.

_____. *The National Security Strategy*, Washington DC: White House, May 2010.

_____. *The National Strategy to Secure Cyberspace*. Washington, DC: White House, February 2003.

_____. *The Physical Protection of Critical Infrastructures and Key Assets*. Washington, DC: White House, February 2003.

U.S. Strategic Command. “U.S. Cyber Command.” Accessed 04 May 2013, http://www.stratcom.mil/factsheets/Cyber_Command/.

Tian, Wei. “Software Bugs Discovered In Chinese Made Applications.” *ChinaDaily.com*, 18 June 2011. Accessed 13 May 2013. http://www.chinadaily.com.cn/cndy/2011-06/18/content_ 12727638.htm.

Vego, Milan N. *Joint Operational Warfare: Theory and Practice*. 2007. Reprint, 2007; U.S. Naval War College, 2009.